

A Game-Theoretical Approach for Finding Optimal Strategies in an Intruder Classification Game*

Lemonia Dritsoula[†], Patrick Loiseau[‡], and John Musacchio[†]

Abstract

We consider a game in which a strategic defender classifies an intruder as spy or spammer. The classification is based on the number of file server and mail server attacks observed during a fixed window. The spammer naively attacks (with a known distribution) his main target: the mail server. The spy strategically selects the number of attacks on his main target: the file server. The defender strategically selects his classification policy: a threshold on the number of file server attacks. We model the interaction of the two players (spy and defender) as a nonzero-sum game: The defender needs to balance missed detections and false alarms in his objective function, while the spy has a tradeoff between attacking the file server more aggressively and increasing the chances of getting caught. We give a characterization of the Nash equilibria in mixed strategies, and demonstrate how the Nash equilibria can be computed in polynomial time. Our characterization gives interesting and non-intuitive insights on the players' strategies at equilibrium: The defender uniformly randomizes between a set of thresholds that includes very large values. The strategy of the spy is a truncated version of the spammer's distribution. We present numerical simulations that validate and illustrate our theoretical results.

1 Introduction

Cybersecurity is important to businesses and individuals. According to a recent study conducted by Symantec [1], the number of cyber attacks and threats has increased during 2011, resulting in lost productivity, reduced revenue, and bad reputation for the associated businesses. Different kinds of attacks (e.g., internal unintentional actions and external malicious ones) should be treated differently and organizations need the security intelligence to respond to all threats rapidly.

*This work was supported by AFOSR grant FA9550-09-1-0049.

[†]Lemonia Dritsoula and John Musacchio are with University of California, Santa Cruz, CA, USA. {lenia, johnm}@soe.ucsc.edu

[‡]Patrick Loiseau is with EURECOM, Sophia-Antipolis, France. Part of this work was done while he was at UC Santa Cruz, CA, USA. patrick.loiseau@eurecom.fr

Since only less than half of organizations are currently pursuing security issues, there is still room for improvement. Our work contributes to the understanding of the interaction between network operators and potential attackers.

In almost every network security situation, the administrator of a network (defender) has limited resources in energy and time. The defender needs to distinguish between different types of attackers (spy or spammer) and decide whether to take actions or not. For example, an attack on a mail server by a spammer (causing at most network congestion) should be treated differently than an attack on a file server (possibly involving identity theft). Therefore, the defender should employ various statistical tests, based on the observed number of file and mail server attacks and decide upon the true type of the attacker. Knowing that a defender is trying to classify attackers, the strategic spy is likely to change the way he attacks in order to make it more difficult to be classified as a spy. In this work, we analyze a simple model of such a classification game and extract key insights.

There exists a growing body of works on the topic of intrusion detection. In a series of papers [2, 3, 4], Alpcan and Başar present a game-theoretic analysis of a security game between an attacker and an intrusion detection system in different scenarios, both in finite and continuous-kernel versions. Our game-theoretic framework focuses on attacker classification, rather than intrusion detection. In the presence of a non-strategic player who is represented with a fixed and known probability distribution, the defender's task of distinguishing the true type of the attacker becomes more challenging. It is also interesting to see how the nonstrategic spammer influences the spy's strategy.

In [5], Patcha and Park model the interaction between a node who might be regular or dangerous and a defender who has some prior probability for the existence of each type in an ad hoc network. They consider a signaling and dynamic game with multiple stages and the players update their beliefs and distributions based on Bayes' rule. On the contrary, our work considers a one-stage game with a fixed duration and we compute the Nash equilibria in mixed strategies.

Chen and Leneutre [6] address the intrusion detection problem in heterogeneous networks consisting of nodes with different non-correlated security assets, in the same way that the file and mail servers are of different importance in our work. They consider a static game with full information and limited attack and monitoring resources. We do not consider such limitations and we assume asymmetric information, since the defender is not aware of the attacker's type.

Bao, Kreidl, and Musacchio [7] also consider an intruder classification game, in which the sequence of attacks is taken into account. While their model has many similarities with ours, we focus on less complex (but still realistic) payoff functions that allow us to go one step further than simulations and analyze the structure of the Nash equilibria.

Gueye, Walrand, and Anantharam [8, 9] have investigated the structure of the Nash equilibria in a network topology game where two adversaries select which links to attack and defend. They consider a special case of nonzero-sum games, in which the different term in the players' payoffs is controlled only by

the one player. In these games, one player optimizes his payoff against the other who has optimized his payoff as well. Such games are easier to analyze than general nonzero-sum games, and they give interesting insights on the strategies of the two players. Our work is using a similar payoff formulation in a different setting: the defender selects a threshold on file server attacks (not a set of links to defend) and there are two different types of attackers.

To the best of our knowledge, [10] is the most relevant work to ours. The authors address the problem of classifying a malicious intruder in the presence of an innocent user. The malicious intruder can perturb his behavior to confuse the classifier and evade detection. But, their work focuses only on one iteration of the game and how each player can once adjust his strategy to optimize his expected payoff, given the optimal strategy of the other player. On the contrary, we provide an algorithm to find the Nash equilibria of the game.

In summary, our contributions are the following. We propose a game-theoretic model to analyze the interactions between two adversaries: a classifier (defender) and a malicious attacker when a nonstrategic spammer is present. We compute the Nash equilibria in polynomial time. We perform numerical experiments that validate the theoretical computation and give non-intuitive insights on the players' strategies.

The rest of the paper is organized as follows. Section 2 describes the game model and underlying assumptions. Section 3 explains how to reduce the complexity of the game and compute the Nash equilibria in polynomial time. Section 4 presents the performance evaluation through numerical experiments and Section 5 concludes the paper.

2 Game Model

The game model is as follows. A network consists of a defender and two servers that are monitored for potential attacks: a File Server (FS) with sensitive data and a Mail Server (MS) with contents of inferior importance. We assume a constant classification window of N time slots (discrete time), during which the defender observes the number of hits on the FS / MS coming from a single attacker. Nature decides the type of the attacker in the network: spy or spammer with probabilities p and $1 - p$ respectively.

The defender is a strategic player and seeks to correctly classify the potential intruder. He selects a threshold T . If he observes T or more hits on the FS, he classifies the attacker as a spy; otherwise as a spammer. The spy's goal is to attack the FS as frequently as possible while evading detection. He is a strategic player and selects the number of FS attacks H to launch.

The spammer is a non-strategic player with a tendency to attack more often the MS to congest the network or annoy the defender. He attacks the FS Z time slots with a known and fixed distribution. For instance, he can be modeled to have a Bernoulli distribution at each time slot with a small per-period probability θ_0 of a hit on the FS.

Notational Conventions:

We use “ $\min[\mathbf{v}]$ ” to denote the minimum element of a vector \mathbf{v} , and “minimize” when we minimize a specific expression over some constraints. We use the *prime* sign ($'$) for transpose of matrices and vectors. All vectors are assumed to be column vectors and are denoted by bold lowercase letters (e.g., $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$). For matrix notation we use capital greek letters (e.g., Λ) and the indicator function is denoted by $\mathbb{1}_{cond}$. It is equal to 1 if “cond” holds and is equal to 0 otherwise. The column vector of ones of length N is denoted by $\mathbf{1}_N$ and the matrix of ones of dimensions $N \times M$ is denoted by $\mathbf{1}_{N \times M}$. An overview of the important parameters is shown in Table 1.

2.1 Spy’s cost function

The spy is detected when $T \leq H$, which incurs a cost of c_d to the spy. Each of the H FS hits gives the spy a benefit of c_a . We assume that the spy gains nothing from attacking the MS. We will work with a cost function for the attacker rather than a payoff function, thus, his overall cost function can be expressed as follows

$$J_A(T, H) = c_d \cdot \mathbb{1}_{T \leq H} - c_a \cdot H.$$

2.2 Defender’s reward function

The defender’s expected reward function depends on the true type of the attacker.

- With probability p the defender faces a spy and classifies him correctly when $T \leq H$. The defender gains c_d for the correct classification of the spy, but loses c_a per FS hit.
- With probability $1 - p$ the defender faces a spammer, who is incorrectly classified as spy with probability $\phi(T) = \Pr\{Z \geq T\}$. The expected false alarm penalty in this case is $c_{fa} \cdot \phi(T)$.

Combining these two scenarios, the defender’s expected payoff is

$$\tilde{U}_D(T, H) = p \cdot (c_d \cdot \mathbb{1}_{T \leq H} - c_a \cdot H) - (1 - p) \cdot c_{fa} \cdot \phi(T).$$

By scaling the above function, we get

$$U_D(T, H) = c_d \cdot \mathbb{1}_{T \leq H} - c_a \cdot H - \mu(T),$$

where $\mu(T) = \frac{1-p}{p} \cdot c_{fa} \cdot \phi(T)$.

Function $\phi(T)$ is decreasing (since it is an complementary cumulative density function) and we also assume that it is strictly decreasing: $\Pr\{Z \geq T\} > \Pr\{Z \geq T + 1\}$.

2.3 Players' interactions

For a fixed observation window N the spy has $N + 1$ available actions (attack the file server $H \in \{0, \dots, N\}$ times), whereas the defender has $N + 2$ available actions (select $T \in \{0, \dots, N + 1\}$ as the classification threshold). A threshold of 0 always results in spy classification (any intruder will attack the FS at least 0 times); a threshold of $N + 1$ always results in spammer classification (a spy cannot attack $N + 1$ times during N).

We model our problem as a nonzero-sum game. However, the defender's payoff is different from the spy's cost function in only one term $\mu(T)$ that depends only on the defenders strategy ($UD(T, H) = JA(T, H) - \mu(T)$). These games are known as almost zero-sum games or quasi zero-sum games. We are interested in Nash equilibria in mixed strategies for the following reason. The spy seeks to select H just below T to evade detection. The defender aims to select a threshold T equal to the attacker's strategy H . Thus the players need to mix between different strategies to make themselves less predictable. The spy chooses a distribution α on the available numbers of FS hits — thus α is a vector of size $N + 1$ with non negative elements that sum to 1. Similarly the defender chooses a distribution β on the collection of possible thresholds T . Thus β is a vector of size $N + 2$.

Let $\tilde{\Lambda}$ be a $(N + 1) \times (N + 2)$ matrix representing the spy's strategies' cost. Since the number of strategies available to each player is not the same, the cost matrix $\tilde{\Lambda}$ is not square. We express the cost matrix of the attacker as

$$\tilde{\Lambda} = c_d \cdot \underbrace{\begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 & 0 \\ \vdots & 1 & \ddots & & \vdots & \vdots \\ \vdots & & \ddots & \ddots & \vdots & \vdots \\ \vdots & & & \ddots & 0 & \vdots \\ 1 & \cdots & \cdots & \cdots & 1 & 0 \end{pmatrix}}_{\tilde{\Lambda}_1} - c_a \cdot \underbrace{\begin{pmatrix} 0 \\ 1 \\ 2 \\ \vdots \\ N-1 \\ N \end{pmatrix}}_{\tilde{\Lambda}_2} \cdot \mathbf{1}'_{N+2}$$

with respective elements $\tilde{\Lambda}_1(i, j) = \mathbb{1}_{j \leq i}$ and $\tilde{\Lambda}_2(i, j) = i$, where $i = \{0, \dots, N\}$ designates the row and $j = \{0, \dots, N + 1\}$ the column.

Each row i of $\tilde{\Lambda}$ corresponds to one of the $N + 1$ possible spy strategies. For instance, row “0” corresponds to spy attacking the FS 0 times (or $H = 0$), row “1” corresponds to spy selecting $H = 1$ and so on. Each column of $\tilde{\Lambda}$ corresponds to one of the $N + 2$ possible defender strategies. For instance, column “0” corresponds to defender selecting $T = 0$ (or always classify as spy). In this case the spy is always detected and loses c_d . The last column “ $N + 1$ ” corresponds to defender selecting $T = N + 1$. Since it is not possible that that spy attacks $N + 1$ times during N time slots, if the defender selects this strategy, the spy is never caught and has zero detection cost. In $\tilde{\Lambda}_2$, every column j (defender strategy) incurs the same benefit to the spy. No matter what the decision threshold is, the impact of the spy's attacks is the same.

Table 1: Main Notations

p	probability for spy	α	spy's mixed strategy
c_d	detection cost	β	def. mixed strategy
c_a	FS attack cost	μ	false alarm cost vector
c_{fa}	false alarm penalty	$\theta(\beta)$	defendability of β
H	spy's strategy (# FS hits)	Λ	cost matrix of spy
T	def. strategy (threshold)	s	first tight inequality
Z	# of FS hits by spammer	f	last tight inequality

Let $\tilde{\Lambda}$ be defined as above, and α, β , be the spy and defender distributions respectively. The attacker cost can be written as $\alpha' \tilde{\Lambda} \beta$ and the defender payoff can be written as $\alpha' \tilde{\Lambda} \beta - \mu' \beta$, where μ is a strictly decreasing vector (component-wise) with μ_i be the i^{th} component of vector μ . Certain computations are simplified by using a matrix with only positive entries. We define

$$\Lambda = \tilde{\Lambda} + (N \cdot c_a + \epsilon) \cdot 1_{(N+1) \times (N+2)},$$

where $1_{(N+1) \times (N+2)}$ is a matrix of all ones of dimension $(N+1) \times (N+2)$ and $\epsilon > 0$. Since α and β must each sum to 1, the expressions $\alpha' \Lambda \beta$ and $\alpha' \Lambda \beta - \mu' \beta$ are respectively the attacker cost and defender payoff shifted by a constant. Adding a constant to the players' payoff does not affect their best responses, thus from here on we will consider these expressions to be the payoff functions of each player.

3 Game-Theoretic Analysis

Nash proved in [14] that every finite game (finite number of players with finite number of actions for each player) has a mixed-strategy Nash equilibrium. Our game is finite, thus it admits a NE in mixed strategies. In a two-player game, the players' strategies α and β are a NE if each player's strategy is a best response to the other player's mixed strategy.

3.1 Best response analysis

We will first prove a series of lemmata that will help us state and prove our main Theorem. We first prove that in a NE, the spy's strategy α minimizes his cost and the defender's strategy β maximizes his payoff.

Lemma 1. *A spy who plays a best response to a defender strategy β , has a cost $\delta = \min[\Lambda \beta]$.*

Proof. For a given defender strategy β and since Λ is positive, the minimum attacker cost is achieved by putting positive probability only on strategies corresponding to the minimum entries of the vector $\Lambda \beta$. Thus the spy's optimal cost is $\delta = \min[\Lambda \beta]$. \square

Definition 1 (Defendability). *The defendability of a mixed strategy β is defined as*

$$\theta(\beta) = \min[\Lambda\beta] - \mu'\beta. \quad (1)$$

It corresponds to the defender's payoff when the attacker plays a best response to β .

The defendability is similar to the notion of vulnerability in [8], that is a measure of how vulnerable a set of links is. An interesting property of the defendability is that it depends only on the defender's strategy and not on the spy's selection of α . This is due to the aforementioned “almost” zero-sum game. We will exploit this property in the subsequent analysis.

In Nash equilibrium, each player in the game selects a best response to the other player's strategies. We show below (Lemma 2) that the defender's best response to any spy's best response maximizes the defendability.

We proved in Lemma 1 that the best response of the spy against any defender strategy β , gives a spy cost $\delta = \min[\Lambda\beta]$. The attacker's optimization problem, subject to the constraint that he limits the defender to the defendability $\theta(\beta)$ takes the following form

Primal with constraints:

$$\begin{aligned} & \underset{\alpha}{\text{minimize}} && \alpha' \Lambda \beta \\ & \text{subject to} && \alpha \geq \mathbf{0}, \mathbf{1}'_{N+1} \cdot \alpha \geq 1, \\ & && \alpha' \Lambda - \mu' \leq \theta(\beta) \cdot \mathbf{1}'_{N+2}. \end{aligned} \quad (2)$$

The last constraint in the above LP comes from the fact that the defender's payoff from any pure strategy in the support of the defender's NE strategy is the same (and equal to the defendability), and at least as good as the payoff from any pure strategy not in the support of his mixed strategy, when the attacker is playing his NE strategy. The dual constrained LP is

Dual with constraints:

$$\begin{aligned} & \underset{\mathbf{y}, z}{\text{maximize}} && (-\mathbf{1}'_{N+2} \cdot \theta(\beta) - \mu') \mathbf{y} + z \\ & \text{subject to} && \mathbf{y} \geq \mathbf{0}, z \geq 0 \\ & && z \cdot \mathbf{1}_{N+1} - \Lambda \mathbf{y} \leq \Lambda \beta. \end{aligned} \quad (3)$$

As we show below, the optimal value of the dual LP given by (3) is equal to δ if and only if β is a maximizer of the function $\theta(\beta)$. If the optimal value was greater than δ , then the attacker would not play a best response against a strategy β , namely we would not be in NE.

Working on (3), the last constraint gives $\Lambda(\beta + \mathbf{y}) \geq z \cdot \mathbf{1}_{N+1}$, and since we seek to maximize a nonnegative z with an upper limit, $z = \min[\Lambda(\beta + \mathbf{y})]$. We note here that since Λ and $(\beta + \mathbf{y})$ are nonnegative matrix and vector respectively, their multiplication is also a nonnegative vector and the above

optimal value for z is valid. With the above substitution for z , we get the following LP

$$\begin{aligned} & \underset{\mathbf{y}}{\text{maximize}} && -\|\mathbf{y}\|\theta(\boldsymbol{\beta}) - \boldsymbol{\mu}'\mathbf{y} + \min[\Lambda(\boldsymbol{\beta} + \mathbf{y})] \\ & \text{subject to} && \mathbf{y} \geq \mathbf{0}, \end{aligned} \quad (4)$$

where we define $\|\mathbf{y}\| = \|\mathbf{y}\|_1 = \sum_{i=0}^{N+1} |y_i|$.

Lemma 2. *In NE, the defender strategy $\boldsymbol{\beta}$ maximizes the defendability $\theta(\boldsymbol{\beta})$.*

Proof. Part I: Suppose that the defender's strategy is $\boldsymbol{\beta}$ such that $\theta(\boldsymbol{\beta}) < \theta(\boldsymbol{\xi})$, where $\boldsymbol{\xi} = \arg \max \theta$. Let $\mathbf{y} = k\boldsymbol{\xi}$, with $k \gg 1$. Then (4) gives

$$\begin{aligned} & \underset{k}{\text{maximize}} && -\|k\boldsymbol{\xi}\|\theta(\boldsymbol{\beta}) - \boldsymbol{\mu}'k\boldsymbol{\xi} + \min[\Lambda(\boldsymbol{\beta} + k\boldsymbol{\xi})] \\ & \text{subject to} && k \gg 1. \end{aligned} \quad (5)$$

Since $k\boldsymbol{\xi} \gg \boldsymbol{\beta}$, $\|\boldsymbol{\xi}\| = 1$ and $\theta(\boldsymbol{\xi}) = \min[\Lambda\boldsymbol{\xi}] - \boldsymbol{\mu}'\boldsymbol{\xi}$, the argument that needs to be maximized in (5) becomes $-k\theta(\boldsymbol{\beta}) + k\theta(\boldsymbol{\xi})$ or $k(\theta(\boldsymbol{\xi}) - \theta(\boldsymbol{\beta}))$. Since $\theta(\boldsymbol{\xi}) > \theta(\boldsymbol{\beta})$, this expression can be made arbitrarily large. Therefore, the optimal value of (4) is infinity. Since the optimal value of the dual problem is unbounded, the initial primal problem is infeasible [12]. Therefore, if the defendability of $\boldsymbol{\beta}$ is not maximal, then $\boldsymbol{\beta}$ is not a NE.

Part II: Suppose that the defender's strategy $\boldsymbol{\beta} \in \arg \max \theta(\boldsymbol{\lambda})$. We show that the optimal values of the attacker's constrained and unconstrained LP problem are the same, i.e., $\delta_{const} = \delta$, where δ_{const} is the optimal value of (2). Since (2) is a minimization problem over a smaller set (extra constraints),

$$\delta_{const} \geq \delta. \quad (6)$$

With the change of variable $\mathbf{q} = \boldsymbol{\beta} + \mathbf{y}$, we transform (4) to the following problem

$$\begin{aligned} & \underset{\mathbf{q}}{\text{maximize}} && -(\|\mathbf{q}\| - \|\boldsymbol{\beta}\|)\theta(\boldsymbol{\beta}) - \boldsymbol{\mu}'(\mathbf{q} - \boldsymbol{\beta}) + \min[\Lambda\mathbf{q}] \\ & \text{subject to} && \mathbf{q} \geq \boldsymbol{\beta}. \end{aligned} \quad (7)$$

We take now a relaxed version of the above problem, where the constraint is $\mathbf{q} \geq \mathbf{0}$ instead of $\mathbf{q} \geq \boldsymbol{\beta}$

$$\underset{\mathbf{q} \geq \mathbf{0}}{\text{maximize}} \{ -(\|\mathbf{q}\| - \|\boldsymbol{\beta}\|)\theta(\boldsymbol{\beta}) - \boldsymbol{\mu}'(\mathbf{q} - \boldsymbol{\beta}) + \min[\Lambda\mathbf{q}] \}.$$

Clearly the optimal value $\delta_{relax-const}$ in the above relaxed maximization problem is greater than or equal to the optimal value δ_{const} of the original problem (7), since we maximize the same objective function over a larger set. Thus

$$\delta_{relax-const} \geq \delta_{const}. \quad (8)$$

Since $\|\beta\| = 1$ and $\delta = \theta(\beta) + \mu'\beta$, from the above relaxed problem we get

$$\underset{q \geq 0}{\text{maximize}} \{ \delta - \|q\| \theta(\beta) + \min[\Lambda q] - \mu'q \}. \quad (9)$$

But $\min[\Lambda q] - \mu'q = \|q\| \cdot \theta(q) \leq \|q\| \cdot \theta(\beta)$, since $\beta \in \arg \max \theta(\lambda)$. Thus, the maximization in (9) always gives an optimal value

$$\delta_{\text{relax-const}} \leq \delta. \quad (10)$$

From (6), (8) and (10) we get $\delta \leq \delta_{\text{const}} \leq \delta_{\text{relax-const}} \leq \delta$, which yields $\delta_{\text{const}} = \delta$. \square

Definition 2 (Tight constraint). *An inequality constraint is tight, if it holds as an equality; otherwise, it is said to be loose.*

Definition 3 (Polyhedron). *A polyhedron is the solution set of a finite number of linear equalities and inequalities.*

Definition 4 (Extreme point). *A point x of a polyhedron is said to be extreme if there is no x' whose set of tight constraints is a strict superset of the set of tight constraints of x .*

Lemma 3. *There exists a defender NE strategy β amongst the extreme points of a polyhedron defined by $\Lambda x \geq \mathbf{1}_{N+1}$, $x \geq \mathbf{0}$.*

Proof. As we proved in Lemma 2, in NE, the defender maximizes the defendability, that is, he solves the following “defendability LP”

$$\begin{aligned} & \underset{\beta, z}{\text{maximize}} && -\mu'\beta + z \\ & \text{subject to} && z \cdot \mathbf{1}_{N+1} \leq \Lambda\beta \\ & && \mathbf{1}'_{N+2} \cdot \beta = 1, \beta \geq \mathbf{0} \end{aligned} \quad (11)$$

The solution for z is $z = \min[\Lambda\beta]$ (finite and positive since Λ positive). The objective is a finite quantity reduced by a positive value ($\mu \geq \mathbf{0}, \beta \geq \mathbf{0}$), thus (11) is bounded. Consider a vector $[\beta; z]$ that is both a solution to (11) and extreme for the inequalities of (11). From the basic theorem of linear programming such a point must exist. Let S be the set of indices of tight inequalities of $\Lambda\beta \geq z \cdot \mathbf{1}_{N+1}$, and P be the set of indices of tight inequalities in $\beta \geq \mathbf{0}$.

Defining $x := \beta/z$, the above constraints become $\Lambda x \geq \mathbf{1}$, $x \geq \mathbf{0}$, and x is a feasible point. The same sets S and P specify the tight inequalities and x is an extreme point of this feasible region. If it is not extreme, then there exists a point \hat{x} with corresponding sets of tight inequalities $\hat{S} \supseteq S$ and $\hat{P} \supseteq P$, one of which is a strict superset. Let $\hat{\beta} = \frac{\hat{x}}{\mathbf{1}'_{N+2} \cdot \hat{x}}$, and $\hat{z} = \min[\Lambda\hat{\beta}]$. It can

be easily shown that $\hat{\beta}$ is a feasible point to the inequalities $\Lambda\beta \geq z\mathbf{1}_{N+1}$, and $\beta \geq \mathbf{0}$: Indeed, $\Lambda\hat{\beta} \geq \min[\Lambda\hat{\beta}] = \hat{z}$, and since $\hat{x} \geq \mathbf{0}$, $\hat{\beta} \geq \mathbf{0}$. It can also be shown that $\hat{\beta}$ has tight inequalities in \hat{S} and \hat{P} . Indeed $\forall j \in \hat{P}, \hat{\beta}_j = 0$ (thus $\hat{\beta}$

has tight inequalities in \hat{P}). $\forall i \in \hat{S}$, $\hat{\mathbf{x}}$ has tight inequalities in \hat{S} , thus $[\Lambda \hat{\mathbf{x}}]_i = \min[\Lambda \hat{\mathbf{x}}] = 1$. We divide the last equation with $\mathbf{1}'_{N+2} \cdot \hat{\mathbf{x}}$ (constant, can get inside the min) and get $[\Lambda(\frac{\hat{\mathbf{x}}}{\mathbf{1}'_{N+2} \cdot \hat{\mathbf{x}}})]_i = \min[\Lambda \frac{\hat{\mathbf{x}}}{\mathbf{1}'_{N+2} \cdot \hat{\mathbf{x}}}]$. But $\frac{\hat{\mathbf{x}}}{\mathbf{1}'_{N+2} \cdot \hat{\mathbf{x}}} = \hat{\beta}$, thus $[\Lambda \hat{\beta}]_i = \min[\Lambda \hat{\beta}]$, so $\hat{\beta}$ has tight inequalities in \hat{S} . Thus $[\hat{\beta}, \hat{z}]$ has a strict superset of tight inequalities to $[\beta; z]$; this is a contradiction with our hypothesis that $[\beta; z]$ was an extreme point. Thus, the defendability is maximized at the extreme points of the polyhedron $\Lambda \mathbf{x} \geq \mathbf{1}_{N+1}$, $\mathbf{x} \geq \mathbf{0}$. Given an extreme point \mathbf{x} , we compute the distribution $\beta = \mathbf{x}/\|\mathbf{x}\|$. Thus, a point $\mathbf{x} = (x_0, \dots, x_{N+1})$ corresponds to a defender's strategy β , after normalizing it. \square

Adding the constant parameter $Nc_a + \epsilon$ to every element of Λ does not change the structure of the Nash equilibria but renders Λ strictly positive. We thus avoid the problems that arise when the minimum element of the vector is zero (infinite solution).

3.2 Form of players' strategies in NE

In this section we show how the NE in mixed strategies for the two players can be computed in polynomial time.

3.2.1 Defender's NE strategy

As we saw in Lemma 3, the best response strategy of the defender is found by looking at the extreme points of the polyhedron $\Lambda \mathbf{x} \geq \mathbf{1}_{N+1}$, $\mathbf{x} \geq \mathbf{0}$. We call the first type "inequality" constraints and the second type "positivity" constraints. We have $N + 1$ "inequality"- and $N + 2$ "positivity" constraints. Writing down the "inequality" constraints, we get

$$\begin{aligned} c_d \cdot x_0 + (Nc_a + \epsilon)\|\mathbf{x}\| &\geq 1 \\ c_d \cdot (x_0 + x_1) + [(N-1)c_a + \epsilon]\|\mathbf{x}\| &\geq 1 \\ &\vdots \\ c_d \cdot (x_0 + x_1 + \dots + x_N) + \epsilon\|\mathbf{x}\| &\geq 1. \end{aligned}$$

Our goal is to eliminate nonextreme points that are not selected by a defender in NE, so that we reduce the number of points we have to check.

Lemma 4. *Two points \mathbf{x}_1 and \mathbf{x}_2 on the polyhedron, with $\|\mathbf{x}_1\| = \|\mathbf{x}_2\|$, correspond to defender NE strategies β_1 and β_2 respectively with $\min[\Lambda \beta_1] = \min[\Lambda \beta_2]$.*

Proof. We showed in Lemma 3 that the equation that needs to be solved in NE is $\Lambda \mathbf{x} \geq \mathbf{1}$, with $\|\mathbf{x}\| = 1/z = 1/\min[\Lambda \beta]$. Thus, if the norm $\|\mathbf{x}\|$ is preserved, the optimal attacker cost $\min[\Lambda \beta]$ is also preserved. Hence $\min[\Lambda \beta_1] = \min[\Lambda \beta_2]$. \square

Lemma 5. *An extreme point \mathbf{x} satisfies at least one tight inequality.*

Proof. If none of the inequalities are tight, we scale the vector \mathbf{x} down until one inequality becomes tight. The new vector's set of tight inequalities is a strict superset of those of the original vector, thus the point with no tight inequalities is not extreme. \square

Lemma 6. *If $\|\mathbf{x}_1\| = \|\mathbf{x}_2\|$ and $\boldsymbol{\mu}'\mathbf{x}_1 < \boldsymbol{\mu}'\mathbf{x}_2$, then \mathbf{x}_1 corresponds to a defender strategy β_1 with a better defendability, i.e., $\theta(\beta_1) > \theta(\beta_2)$.*

Proof. Since $\|\mathbf{x}_1\| = \|\mathbf{x}_2\|$, $\min[\Lambda\beta_1] = \min[\Lambda\beta_2]$ (Lemma 4). Combining the above result with the definition of the defendability we get

$$\begin{aligned}\theta(\beta_1) - \theta(\beta_2) &= \min[\Lambda\beta_1] - \boldsymbol{\mu}'\beta_1 - (\min[\Lambda\beta_2] - \boldsymbol{\mu}'\beta_2) \\ &= \boldsymbol{\mu}'\beta_2 - \boldsymbol{\mu}'\beta_1.\end{aligned}$$

Since $\boldsymbol{\mu}'\mathbf{x}_1 < \boldsymbol{\mu}'\mathbf{x}_2$, the point \mathbf{x}_1 corresponds to a defender strategy β_1 with a smaller false alarm cost, $\boldsymbol{\mu}'\beta_1 < \boldsymbol{\mu}'\beta_2$. Hence $\theta(\beta_1) > \theta(\beta_2)$. \square

Lemma 7. *An extreme point \mathbf{x} corresponding to a defender NE strategy β satisfies exactly one contiguous set (of indices) of tight inequalities.*

Proof. An extreme point satisfies at least one tight inequality (Lemma 5). Suppose there are two tight inequalities with indices s and f , with $f > s$, and that there is at least one loose inequality (with index k) between s and f . Since k is loose, it should be that $x_k \geq \frac{c_a}{c_d}\|\mathbf{x}\| > 0$ (after subtracting the loose inequality from the previous tight one). We make the following transformation

$$\hat{x}_i = \begin{cases} x_i & \text{for } i \in \{0, \dots, k-1\} \cup \{k+2, \dots, N+1\} \\ x_i - \epsilon_1 & \text{for } i = k \\ x_i + \epsilon_1 & \text{for } i = k+1, \end{cases} \quad (12)$$

where $\epsilon_1 > 0$ is small enough so that $\hat{x}_i \geq \frac{c_a}{c_d}\|\hat{\mathbf{x}}\|$.

The transformation preserves the norm ($\|\mathbf{x}\| = \|\hat{\mathbf{x}}\|$), but $\boldsymbol{\mu}'\mathbf{x} > \boldsymbol{\mu}'\hat{\mathbf{x}}$. The latter comes from the fact that $\boldsymbol{\mu}'(\mathbf{x} - \hat{\mathbf{x}}) = \mu_k \cdot (x_k - \hat{x}_k) + \mu_{k+1} \cdot (x_{k+1} - \hat{x}_{k+1}) = \mu_k \cdot \epsilon_1 + \mu_{k+1} \cdot (-\epsilon_1) = \epsilon_1 \cdot (\mu_k - \mu_{k+1}) > 0$, since $\boldsymbol{\mu}$ is a strictly decreasing vector (component-wise). Thus, from Lemma 6, $\hat{\mathbf{x}}$ corresponds to a defender strategy with a better defendability. If there are more than one loose inequalities, we can iteratively make the above transformation until the point $\hat{\mathbf{x}}$ has a unique contiguous block of tight inequalities, in which case $\hat{\mathbf{x}}$ corresponds a defender NE strategy (a defender's unilateral change of strategy would not result in a better defendability). \square

Let s and f be the indices of the first and last tight inequalities respectively.

Lemma 8. *An extreme point \mathbf{x} that corresponds to a defender NE strategy β has zeros before s and after $f+1$, i.e.,*

$$x_i = 0, \forall i \in \{0, \dots, s-1\} \cup \{f+2, \dots, N+1\}.$$

Proof. We first show that $x_i = 0, \forall i < s$. If $\exists i \in \{0, \dots, s-1\}$, s.t. $x_i > 0$, we reduce x_i to \hat{x}_i until either $\hat{x}_i = 0$ or until the i^{th} (previously loose) inequality becomes tight, and increase x_{i+1} by the same amount. We maintain $\|\mathbf{x}\|$ constant, but we get one more tight constraint. Thus the original point is not extreme, as we can find another point whose tight constraints is a strict superset of those of the original.

We now show that $x_i = 0, \forall i > f+1$. If $\exists i \in \{f+2, \dots, N+1\}$, s.t. $x_i > 0$, we reduce x_i until $\hat{x}_i = 0$, and increase x_{f+1} by the same amount. The previously loose $(f+1)^{\text{th}}$ inequality is made looser, and we keep the norm $\|\mathbf{x}\|$ constant, but $\hat{\mathbf{x}}$ has one more tight constraint, thus \mathbf{x} was not extreme. \square

Lemma 9. *In any Nash equilibrium, $f = N$.*

Proof. Suppose that $f < N$. Subtracting the tight inequality f from the loose inequality $f+1$, we get $x_{f+1} > x_m$, where $x_m = \frac{c_a}{c_d} \|\mathbf{x}\|$. We make the following transformation

$$\hat{x}_i = \begin{cases} x_i & \text{for } i \in \{0, \dots, f\} \cup \{f+3, \dots, N+1\} \\ x_m & \text{for } i = f+1 \\ x_{f+1} - x_m & \text{for } i = f+2. \end{cases} \quad (13)$$

With the above transformation we get

$$\begin{aligned} \boldsymbol{\mu}'(\hat{\mathbf{x}} - \mathbf{x}) &= \mu_{f+1} \cdot (\hat{x}_{f+1} - x_{f+1}) + \mu_{f+2} \cdot (\hat{x}_{f+2} - x_{f+2}) \\ &= \mu_{f+1} \cdot (x_m - x_{f+1}) + \mu_{f+2} \cdot (x_{f+1} - x_m - 0) \\ &= (x_{f+1} - x_m) \cdot (\mu_{f+2} - \mu_{f+1}) \\ &< 0, \end{aligned}$$

since $x_{f+2} = 0$, $x_{f+1} > x_m$, and $\boldsymbol{\mu}$ is a strictly decreasing vector ($\mu_{f+2} < \mu_{f+1}$). Hence, for the new point $\hat{\mathbf{x}}$, it holds that $\|\hat{\mathbf{x}}\| = \|\mathbf{x}\|$, but $\boldsymbol{\mu}'\hat{\mathbf{x}} < \boldsymbol{\mu}'\mathbf{x}$. Thus from Lemma 6 point $\hat{\mathbf{x}}$ corresponds to a defender NE strategy with a better defendability. We can continue making the above transformation until $f = N$, when the defender's payoff cannot be maximized by a unilateral deviation. Hence, in any Nash Equilibrium, $f = N$. \square

Lemma 10. *An extreme point \mathbf{x} that corresponds to a defender NE strategy $\boldsymbol{\beta}$ cannot have both $x_s > 0$ and $x_{N+1} > 0$.*

Proof. In Lemmata 7–9, we proved that an extreme point \mathbf{x} that corresponds to a defender NE strategy satisfies a contiguous block of tight inequalities with nonzero components between s through $N+1$. We make the following transformation

$$\hat{x}_i = \begin{cases} \gamma \cdot x_i & \forall i \in \{0, \dots, s-1\} \cup \{s+1, \dots, N\} \\ 0 & \text{for } i = s \\ \gamma \cdot (x_s + x_i) & \text{for } i = N+1, \end{cases} \quad (14)$$

Table 2: Defender's strategy in NE ($\beta_m = c_a/c_d$)

#	...	β_s	β_{s+1}	...	β_N	β_{N+1}
1.	0	0	β_m	β_m	β_m	$1 - (N - s)\beta_m$
2.	0	$1 - (N - s)\beta_m$	β_m	β_m	β_m	0

with $\gamma = \frac{1}{1 - c_d \cdot x_s}$ or, $\gamma = \frac{1}{\|\mathbf{x}\|[(N - s)c_a + \epsilon]}$. The definition of γ is such that the s^{th} inequality is still tight after the transformation, i.e.,

$$\gamma \cdot (c_d \cdot 0 + [(N - s)c_a + \epsilon]\|\mathbf{x}\|) = 1.$$

The loose inequalities before s become looser with the scaling with γ ($\gamma > 1$), whereas the previously tight inequalities $s + 1$ through N are still tight. Indeed, after the above transformation, any previously tight inequality with index $k \in \{s + 1, \dots, N\}$ gives

$$\begin{aligned} & \gamma (c_d \cdot (0 + x_{s+1} + \dots + x_k) + [(N - s - k)c_a + \epsilon]\|\mathbf{x}\|) \\ &= \gamma (c_d(x_s + x_{s+1} + \dots + x_k) + [(N - s - k)c_a + \epsilon]\|\mathbf{x}\|) - \gamma c_d x_s \\ & \text{(after subtracting and adding } \gamma \cdot c_d x_s) \\ &= \gamma - \gamma \cdot c_d x_s \text{ (the } (s + 1)^{\text{th}} \text{ inequality was tight before)} \\ &= 1 \text{ (from the definition of } \gamma). \end{aligned}$$

With the above transformation, we get an extra tight constraint ($x_s = 0$), thus the previous point was not extreme. \square

Lemma 11. *For an extreme point \mathbf{x} that corresponds to a defender NE strategy β , we only have two possible combinations*

1. $(0, \dots, 0, x_s = 0, x_{s+1} = \dots = x_N = x_m, x_{N+1} \geq 0)$
2. $(0, \dots, 0, x_s > 0, x_{s+1} = \dots = x_N = x_m, x_{N+1} = 0)$, where $x_m = \frac{c_a}{c_d}\|\mathbf{x}\|$.

Proof. From Lemma 7, the inequalities s through N are tight. Subtracting any tight inequality k , $k \in \{s + 1, \dots, N\}$ from the first tight inequality (s^{th}), gives $x_k = x_m$, with $x_m = \frac{c_a}{c_d}\|\mathbf{x}\|$. Also, from Lemma 8, $x_i = 0, \forall i \in \{0, \dots, s - 1\}$. From Lemma 10, the combination $x_s > 0$ and $x_{N+1} > 0$ is not possible, thus the only possible forms of extreme points \mathbf{x} that correspond to a defender NE strategies are the ones described above. \square

We can now state and prove our main Theorem.

Theorem. *In any Nash equilibrium the defender's strategy β maximizes the defendability (1). A maximizing value of β exists amongst one of the two forms in Table 2 for some s . If there is only one maximizing β amongst vectors of the form in Table 2, then the Nash equilibrium is unique.*

Proof. The first statement of the Theorem is a direct consequence of Lemma 2. Combining the results of Lemmata 3 and 11, we can prove the second statement. In the first type, when $x_s = 0$, the point \mathbf{x} corresponds to a defender NE strategy β with $\|\beta\| = 1$, thus $\beta_{N+1} = 1 - (N - s) \cdot \beta_m$ or $\beta_{N+1} = 0$ and equivalently for the second type, where $x_s > 0$, we have $\beta_s = 1 - (N - s) \cdot \beta_m$, with $\beta_m = c_a/c_d$. Hence, there exists a Nash equilibrium in which the defender's strategy β has one of the two forms in Table 2. \square

In the case that $(N - s)\beta_m = 1$, then both cases give the same NE strategy $\beta = (0, \dots, \beta_1 = \dots = \beta_N = \beta_m, 0)$. Then, $(N - s)c_a = c_d$ and since $s \geq 0$, the condition that needs to be satisfied is $c_d \leq Nc_a$.

If the defendability LP (11) produces a unique maximizer β , then only one of the above cases will maximize the defendability and therefore the Nash equilibrium will be unique. In the case that the solution of (11) is not unique, we could prevent ties between extreme points that vary in s by a small perturbation to the problem (e.g., by modifying the function μ such that it produces a unique maximizer of the defendability).

3.2.2 Attacker's NE strategy

In mixed-strategies NE, each player is indifferent among the strategies in their support. Thus, any pure strategy i with $\beta_i = 1$ in the defender's support yields the same (maximum) payoff θ to the defender in NE.

We have proved that in any Nash equilibrium, the defender is playing with a mix of strategies β that maximizes defendability. If there exists a unique maximizer β of the defendability and $\hat{\theta}$ is the maximum defendability, the attacker's NE strategy α is uniquely derived by the following procedure. First construct a sub matrix of Λ that we call Λ_r , by keeping only the columns that correspond to the support of the defender's strategy (s through N , or $s + 1$ through $N + 1$, or $s + 1$ through N) and rows that correspond to the support of the attacker's strategy (s through N). The defender assigns weight to $\{\beta_{\hat{s}}, \dots, \beta_{N+1}\}$, according to Table 2, where \hat{s} optimizes the defendability. The attacker assigns positive weight to $\{\alpha_{\hat{s}}, \dots, \alpha_N\}$ according to the equations

$$\alpha' = [0; \alpha'_r] \quad (15)$$

$$\alpha'_r = (\hat{\theta} \cdot \mathbf{1}' + \mu'_r) \cdot \Lambda_r^{-1}. \quad (16)$$

This procedure gives a unique α . This α must be a valid probability distribution (sum to one and have nonnegative elements) for if otherwise, it would contradict Nash's existence theorem.

If there are multiple choices of β that maximize the defendability (and this can happen either when both cases in Table 2 or various selections for s in the same case, give the same maximal defendability), from Nash's existence theorem (and our analysis), at least one of β will yield an α with the above procedure that corresponds to a valid probability distribution.

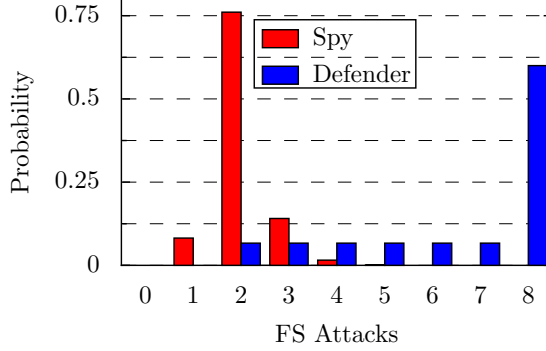


Figure 1: (Type I) Players's best responses in NE for $N = 7$, $\theta_0 = 0.1$, $c_d = 15$, $c_a = 1$, $c_{fa} = 23$, $p = 0.2$.

The complexity to find the NE is polynomial: $O(N^2)$ to find the defendability, $O(N)$ for each case, and $O(N^2 \log N)$ to invert matrix Λ_r . Since we have proved that β has a contiguous set of positive elements, we have reduced all the other degrees of freedom and we make only $N + 1$ computations for each case to find the optimal s . For the special case that $c_d \leq N \cdot c_a$, the two forms coincide and result in the same NE.

4 Numerical Results/Simulations

We conducted various experiments for different sets of parameters N , c_a , c_d , c_{fa} , and p , assuming that the spammer attacks with Bernoulli distribution with parameter θ_0 . We followed the procedure described above to calculate the strategies of both players at equilibrium. To validate our theoretical results, we used Gambit software [13].

Fig. 1 illustrates the first possible type for $N = 7$. As we can see, all the middle points are given the same weight $\beta_m = c_a/c_d = 0.0667$, $\beta_s = 0$ and $\beta_{N+1} > \beta_m$. There exists a Nash equilibrium that matches the first row of Table 2 with $s = 1$.

Fig. 2 represents the second type of Nash equilibrium strategies for $N = 7$. As we can see, all the middle points are given the same weight $\beta_m = c_a/c_d = 0.1$, but here $\beta_s > \beta_m$ ($s = 0$) and $\beta_{N+1} = 0$. Note that as p increases, larger weight is given to the smallest threshold, in order to detect the most-probable-to-exist spy.

In both figures we observe that the defender gives positive weight on larger thresholds and is not focused on a range around $N\theta_0$. Every pure strategy (threshold) in the support of the defender's NE strategy must give the defender the same payoff. The attacker's NE strategy α is such that he makes the defender's NE payoff for high thresholds the same as for lower ones. This is why the defender gives positive weight to higher thresholds, even when the

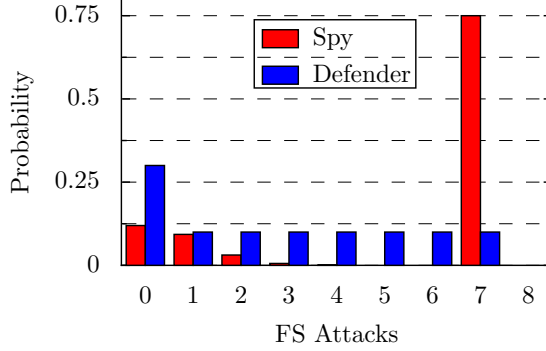


Figure 2: (Type II) Players's best responses in NE for $N = 7$, $\theta_0 = 0.1$, $c_d = 10$, $c_a = 1$, $c_{fa} = 10$, $p = 0.8$.

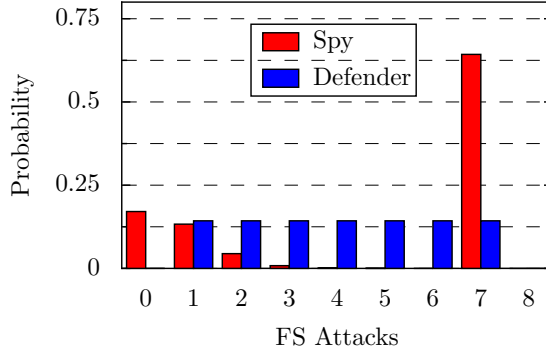


Figure 3: Type I-II: Defender is uniform when $c_d \leq N \cdot c_a$. Other parameters are $N = 7$, $\theta_0 = 0.1$, $c_a = 1$, $c_{fa} = 10$, $p = 0.8$, $c_d = 7$.

probability that the spy will attack more than the threshold value is low.

Fig. 3 depicts the NE in which both forms coincide, i.e., when $c_d \leq N \cdot c_a$. As we can see, the defender NE strategy is uniform and he never classifies the attacker always as spy or always as spammer.

Our simulation results indicated a match between the spy and spammer. In NE, all threshold strategies in the support of the defender give the same payoff. When the defender selects a slightly larger threshold in his support, the decrease in the false alarm cost matches the increase in the misdetection cost, i.e., $\Pr\{H = T\} = \frac{c_{fa}}{c_d} \frac{1-p}{p} \Pr\{Z = T\}$. Hence, the spy's NE strategy is a scaled version of the spammer's distribution. For the spammer strategies that are outside the spy's support in NE, the spy gives zero weight. The spy's NE strategy is a truncated version of the spammer's distribution, as Fig. 4 shows. When either of p or c_d or c_{fa} is large enough, the spy could also put some weight on the “always attack” strategy — and so that part of his strategy doesn't look like a truncated spammer distribution.

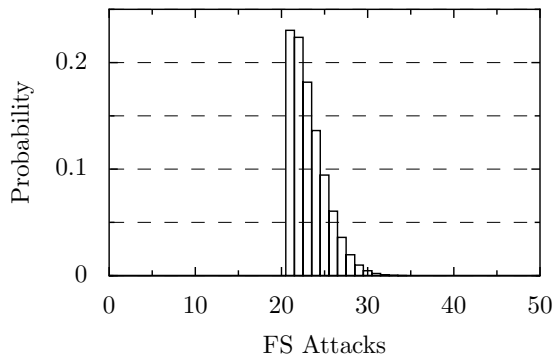


Figure 4: Spy’s NE strategy is a truncated version of spammer’s distribution. Parameters: $N = 50$, $\theta_0 = 0.4$, $c_d = c_{fa} = 142$, $c_a = 1$, $p = 0.3$.

5 Conclusion

We investigated a classification game, where a network administrator (defender) seeks to classify an attacker as a strategic spy or a naive spammer. We showed that by taking advantage of the structure of the payoff formulation, we can characterize and anticipate the structure of the best response strategies of the two players in polynomial time. Our experimental results coincide with the theoretically expected ones: The structure of the cost matrix of the spy leads to only two forms of defender’s strategies in NE. There is a relationship between the spammer’s distribution and the spy’s NE strategy. Furthermore, the defender NE strategy includes a contiguous set of thresholds that always include large values. If the parameters of the game satisfy a certain condition, the defender is uniformly randomizing among a set of thresholds.

References

- [1] “State of Security Survey – Global Findings,” Symantec, 2011.
- [2] T. Alpcan, and T. Başar, “A Game Theoretic Approach to Decision and Analysis in Network Intrusion Detection,” in *Proc. of the 42nd IEEE Conf. Decision and Control*, December 2003, pp. 2595–2600.
- [3] T. Alpcan, and T. Basar, “A Game Theoretic Analysis of Intrusion Detection in Access Control Systems,” in *Proc. of the 43rd IEEE Conf. Decision and Control*, 2004, pp. 1568–1573.
- [4] T. Alpcan, and T. Basar, “An Intrusion Detection Game with Limited Observations,” in *Proc. of the 12th Int. Symp. Dynamic Games and Applications*, 2006.

- [5] A. Patcha and J. M. Park, "A game theoretic formulation for intrusion detection in mobile ad hoc networks," *International Journal of Network Security*, Vol. 2, No. 2, pp. 146-15, Mar. 2006.
- [6] L. Chen, J. Leneutre, "A game theoretical framework on intrusion detection in heterogeneous networks," in *IEEE Transactions on Information Forensics and Security*, v.4 n.2, pp.165-178, June 2009.
- [7] N. Bao, O. P. Kreidl, and J. Musacchio, "A Network Security Classification Game," in *GameNets*, April 2011.
- [8] A. Gueye, J. C. Walrand, and V. Anantharam, "A Network Topology Design Game: How to Choose Communication Links in an Adversarial Environment?," in *GameNets*, April 2011.
- [9] A. Gueye, "A Game Theoretical Approach to Communication Security," PhD dissertation. University of California, Berkeley, Electrical Engineering and Computer Sciences, March 2011.
- [10] N. Dalvi, P. Domingos, Mausam, S. Sanghai, and D. Verma, "Adversarial classification," in *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD)*, pp. 99–108, 2004.
- [11] S. Boyd and L. Vandenberghe, "Convex Optimization." 2004.
- [12] D. G. Luenberger, "Linear and Nonlinear Programming." 2nd ed. Addison-Wesley, 1984.
- [13] Gambit, "Gambit game theory analysis software and tools," <http://www.hss.caltech.edu/gambit>, 2002.
- [14] J. Nash, "Non-Cooperative Games," *The Annals of Mathematics* 54(2):286-295, 1951.